Summer Research Project: Shared Memory Security on Heterogeneous SoC Platforms

Faculty Supervisor: Selcuk Kose

This project investigates hardware-level security vulnerabilities arising from shared memory architectures in heterogeneous System-on-Chip (SoC) platforms, with a primary focus on the NVIDIA Jetson AGX Orin. As AI accelerators, CPUs, and specialized engines increasingly share memory resources on a single die, new attack surfaces emerge that traditional software-only defenses cannot fully address.

The core technical objective is to characterize and demonstrate information leakage channels that exploit shared Last-Level Cache (LLC) or DRAM row-buffer contention between isolated execution contexts on the AGX Orin—or a comparable shared-memory SoC. The student will study how concurrent workloads running on different processing units (CPU clusters, GPU, Deep Learning Accelerator) can inadvertently expose timing side-channels, and will prototype a proof-of-concept measurement framework that quantifies leakage bandwidth under realistic AI inference workloads. The project additionally explores potential countermeasures including cache partitioning, memory access scheduling, and hardware isolation primitives available on modern embedded SoC platforms.

Through this project, the student will gain hands-on experience with embedded Linux, hardware performance counters, and low-level memory profiling tools. They will learn fundamental concepts in computer architecture security including memory bus contention, and the interplay between microarchitectural features and security guarantees. The project provides exposure to real AI-edge hardware while building practical skills in system programming, experimental measurement, and security analysis.

Prerequisites: Basic knowledge of computer architecture and operating systems. Familiarity with C/C++ or Python is required. Prior exposure to computer security or hardware design is beneficial but not mandatory.

Learning Outcomes: Hardware security analysis, shared memory microarchitecture, side-channel measurement methodology, embedded Linux system programming, technical documentation and research communication.